

III. REMARKS

In the Official Action, claims 19, 21, 23, 27-28, 36, 48, 55-59, 61-62, 65, 68, 74, 77-79, 81-82, 84-87, 90-91, 93-94, 96, 122-124, 128, 132-134, 136-139, 142 and 148, 152-153, and 156 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sasuta et al. (U.S. Patent 5,502,767) in view of Talbot (U.S. Patent 4,555,805).

Claims 24-26, 63-64 and 135 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sasuta et al. and Talbot and further in view of Billstrom et al. (U.S. Patent 5,590,133).

Claims 31-34, 66-67, 69, 97, and 143-146 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sasuta et al. and Talbot and further in view of Lewis et al. (U.S. Patent 6,192,255).

Claims 35 and 70 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sasuta et al. and Talbot and further in view of Kniffin et al. (U.S. Patent 6,072,402).

Claims 44-47 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sasuta et al. and Talbot and further in view of Serbetciouglu (U.S. Patent 5,719,918).

Claims 37-43, 75-76, 80, 88-89, 92, 125-127, 129-131, 149-151, and 154-155 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sasuta et al. and Talbot and further in view of Kennedy et al., European Patent 0 680 171.

Claims 49-53 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sasuta et al. and Talbot in view of Kennedy and Lewis (European Patent 0 680 171 and U.S. Patent 6,192,255 respectively).

Claims 140-141 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sasuta et al. and Talbot in view of Raith (U.S. Patent 5,237,612).

Claim 147 is rejected under 35 U.S.C. 103(a) as being unpatentable over Sasuta et al. and Talbot in view of Fujiwara et al. (U.S. Patent 5,266,947).

The examiner notes that the arguments presented in the prior response are moot in view of new grounds of rejection based on the teachings of the new reference Sasuta in combination with previously cited art.

Various amendments are made to improve consistency between the terminology of the claims and the terminology found in the specification.

The *cipher mode control signal* is amended to *cipher mode command message*.

In claim 19

– “*monitoring at the mobile station signals ... the cipher mode control signal for setting the mobile station in an enciphered mode of communication*” is amended to read “*monitoring at the mobile station control signals ... the cipher mode command message requesting the mobile station to start enciphering*”. See US publication 2001/0014942, paragraph 0021, lines 4 – 8.

“*responsive to reception of a cipher mode control signal from the mobile communication network, setting the mobile station into an enciphered mode of communication and indicating to a user of the mobile station that the mobile communication network is configured to use an enciphered mode of communication*” is amended to read “*responsive to detection of a cipher mode command message in the monitored control signals from the mobile communication network, starting enciphering in the mobile station and indicating to a user of the mobile station that the mobile communication network operating in an enciphered mode of communication, using a cipher mode indicator provided in the mobile station*”. Here the language has been amended to clarify that the indication provided to a user of the mobile station provides an indication that the network is actually operating in an enciphered mode, rather than simply being

configured to use an enciphered mode. Furthermore, this indication is provided "by means of a cipher mode indicator provided in the mobile station". Support for this latter amendment can be found from the technical specification as a whole, for example paragraphs 0021 to 0024. We believe this may help provide / emphasise the distinction between the present invention and the Examiner's reasoning concerning "indications" provided according to the Talbot patent. A separate method and apparatus claim has now been added to cover the situation in which the cipher mode indicator is not actually a part of the mobile station. This proved a simpler solution than trying to cover both embodiments with the same independent claim, enabling the details of the technical description to be reflected more straightforwardly in the dependent claims.

As to the amendment made to claim 21 it is similar to that made in the independent claim and is intended to clarify that the indication provided indicates the actual operating mode of the network, rather than simply is capability to operate in certain ciphering modes. As in the independent claim, the reference to the "cipher mode indicator" is intended to emphasize that the indication is provided in real-time, rather than taking the form of a later "indication" e.g. from billing information according to the Examiner's interpretation of the Talbot patent.

Claim 36 is amended for closer correspondence with language used in the technical description (see US publication, paragraph 0022, lines 1 to 7).

Claim 37 is amended for closer correspondence with the language used in the technical description (see US publication, paragraph 0022, lines 7 to 10).

Claim 38 is amended for greater correspondence with the language used in the technical specification (see paragraph 0022 of US publication 2001/0014942, lines 10 to 14).

In claim 39 the reference to the mobile station comprising a cipher mode indicator has been removed from this claim since the presence of a cipher mode indicator is now

explicitly mentioned in the independent claim. Claim 39 is further amended for closer correspondence with the language used in the technical specification (see US publication, paragraph 0022, lines 14 to 17).

Claim 40 is amended for closer correspondence with the language used in the technical specification (see US publication, paragraph 0023).

Claim 41 is amended for closer correspondence with the language used in the technical specification (c.f. claim 39).

Claim 42 is amended for closer correspondence with the language used in the technical specification (see US publication, paragraph 0024, lines 1 to 7).

Claim 43 is amended for closer correspondence with the language used in the technical specification (c.f. claims 39 and 41).

In claims 66 to 70 the means plus function language has been amended. Support for the amendment can be found from the US publication as follows:

Claim 66: paragraph 0028, which states that the apparatus comprises a visual display unit, in combination with paragraph 0030, lines 7 to 14, which describe how voltages are supplied to the visual display unit when the cipher mode is "on" or "off".

Claim 67: paragraph 0039.

Claim 68: paragraph 0010, lines 4 to 7, for example.

Claim 69: paragraph 0022, lines 17 to 20 and paragraph 0030, lines 14 to 23, for example.

Claim 70: paragraph 0040.

Also claims 74 to 81 have been amended for closer correspondence with the language used in the technical description.

Claims 82, 85 and 94 are amended in accordance with independent method claim 19 and independent apparatus claim 59.

Claims 86 to 93 are amended to correspond with claims 74 to 81, respectively.

As to the amendments of claim 122

the definition "*a cipher indicator memory block comprising a cipher indication data field, the cipher indication data field having a value representative of an enciphering mode used in communication between the mobile communication network and the mobile station*" is supported by the US publication, paragraph 0021;

the definition "*a cipher mode indicator for indicating a ciphering mode to a user of the mobile station*" is supported by the US publication, paragraph 0008, lines 8 & 9 + paragraph 0022, lines 14 to 17;

the definition "*a user interface block*" is supported by US publication, paragraphs 0022, 0023 and 0024. The user interface block is first mentioned in paragraph 0022, lines 10 & 11 and its operation in further embodiments of the invention is also described in paragraphs 0023 and 0024;

the definition "*the user interface block being configured to set the cipher mode indicator into a mode corresponding to the value of the cipher indication data field*" is supported by the US publication, paragraph 0022, lines 14 to 17. Although these lines of text state that the user interface block "sets the cipher indicator to the mode corresponding to the *ciphering data*", the earlier part of paragraph 0022 makes it clear that the "ciphering data" is effectively the value held in the cipher indication data field.

Claim 132 is amended to correspond with claim 122.

The subject matter of claims 127, 129 and 131 is now incorporated into the independent claim.

With respect to the rejections under 35 U.S.C. 103, various ones of the claims are amended and the following argument is presented to distinguish the claimed subject matter from the teachings of the cited art, considered individually and in combination, thereby to overcome the rejections and to show the presence of allowable subject matter in the claims.

Claims 19, 21, 27, 35-43, 58-59, 61, 66-70, 74-82, 84-94, 96, 122, 124-126, 128, 130, 132, 136-137, and 147-156 have been amended.

Claims 27, 49-53, 65, 97, 123, 127, 129 and 131 have been cancelled.

As a result, claims 19, 21, 23-26, 28, 31-48, 55-59, 61-64, 66-70, 74-82, 84-94, 96, 122, 124-126, 128, 130, 132, and 133-156 are now pending in the application.

In the following, the Applicant presents arguments in favor of the patentability of the currently pending independent claims, that is, claims 19, 59, 82, 85, 94, 122, 132, 136, and 156. As dependent claims include all the features of the claim(s) from which they depend, it is the Applicant's view that demonstrating the patentability of the independent claims should also be sufficient to demonstrate the patentability of the dependent claims.

Independent claims 19, 59, 82, 85, 94, 122, 132, 136, 156 are rejected in point 6 of the Official Action under 35 U.S.C. 103(a) as being unpatentable over Sasuta et al. (U.S. Patent 5,502,767) in view of Talbot (U.S. Patent 4,555,805). Thus, the Applicant's arguments will focus on distinguishing independent claims 19, 59, 82, 85, 94, 122, 132, 136, and 156 from the teachings of Sasuta and Talbot in combination.

Before considering the applicability of combining the references to support the rejections under 35 U.S.C. 103, there is presented an analysis of the teachings of the individual references.

U.S. Patent 5,502,767 (Sasuta et al.)

Sasuta et al. concerns the synchronization of secure information on a control channel of a secure radio trunking communication system.

More specifically, the Sasuta patent concerns a secure radio trunking communication system in which transmitted / received information can be protected using an encryption algorithm. According to Sasuta, such a system typically comprises a controller that is operably connected to a predetermined number of repeaters, providing communication channels to a plurality of secure communication units, one of the communication channels being used as a control channel, the other communication channels being used as "working" channels (column 1, lines 15 to 27). The Applicant interprets a "working channel" in Sasuta's terminology as a radio communication channel that is used for communicating user data (e.g. voice data) between a particular secure communication unit and the fixed part of the trunking communication system.

Sasuta further discloses that in order to ensure information in such systems is communicated securely, the information on the working channels and the control channel may be protected with encryption. In particular, protecting information on the control channel ensures that the system is protected from malicious parties copying and replaying the control information on the control channel (column 1, lines 29 to 35). According to Sasuta, in a secure radio trunking system, the controller maintains secure information that includes control encryption information (CEI) and control encryption parameters (CEP) to encrypt / decrypt information on the control channel and working encryption parameters to encrypt / decrypt information on the working channels (column 1, lines 35 to 41). Furthermore, in such a system, the encryption parameters (CEP) used on the control channel may include components that change with time and the controller may be configured to periodically transmit the encryption parameters on the control channel in order to update the CEP and maintain CEP synchronization between the controller and the secure communication units operating within the system (column 1, lines 41 to 52).

While on the control channel, a secure communication unit will thus receive periodic CEP updates. However, when the controller assigns the secure communication unit to a working channel, the secure communication unit is no longer able to receive the periodic updates (column 1, lines 52 to 56). As a result, therefore, when returning to the control channel, the CEP stored in the secure communication unit may not be synchronized with the CEP at the controller and the secure communication unit may no longer be able to communicate on the control channel (column 1, lines 56 to 59).

Sasuta proposes a solution to this problem whereby the controller sends periodic CEP updates on the working channel when the secure communication unit is assigned a working channel, thereby maintaining synchronization of the encryption parameters for the control channel while the secure communication unit is communicating on the working channel (column 2, line 64 to column 3, line 6). The control channel encryption parameters are therefore up to date when the secure communication unit switches back to the control channel.

U.S. Patent 4,555,805 (Talbot)

The Talbot patent concerns a communication system that includes a central station and a plurality of remote stations, in which signalling transmissions for establishing a communications channel between the central and remote stations are conducted in a clear (unciphered) mode and subsequent voice transmissions between the central and remote stations are conducted in a secure (enciphered) mode.

Each remote station has a unique code assigned to it. The remote station uses the assigned code to decipher incoming enciphered voice transmissions from the central station. The central station uses the same code to encipher outgoing voice transmissions to the remote station. The unique code may also be used by the remote station to encipher outgoing voice transmissions and by the central station to decipher incoming voice transmissions from the remote station. Alternatively, all remote station

outgoing voice transmissions may be enciphered with a code common to all remote stations, the same code then being used by the central station for deciphering incoming voice transmissions from the remote stations.

The central station can automatically, or in response to a specific request for secure service, switch its equipment to the secure mode upon completion of the channel establishing signalling transmissions and can control remote station switching to the secure mode by sending an enciphered voice transmission to the remote station which responds to receipt thereof by switching to the secure mode (see abstract).

Argumentation With Regard to Rejection of Independent Claims 19, 59, 82, 85, 94, 122, 132, 136, and 156

This argument is presented to show that an attempted combination of the teachings of the primary reference Sasuta with the teachings of Talbot does not support the rejections under 35 U.S.C. 103.

As described above, the Sasuta patent is concerned with ensuring that synchronization of encryption parameters **for an enciphered control channel** is maintained when a secure communication unit switches to a working (communication) channel for a particular period of time. By transmitting the control channel encryption parameters (CEP) on the working channel, the radio trunking communication system proposed by Sasuta enables the control channel encryption parameters to be kept up to date while the secure communication unit is communicating on the working channel. This, in turn, ensures that the correct encryption parameters are available at the secure communication unit for use in communication on the control channel when the secure communication unit switches back to the control channel.

Talbot, on the other hand, relates to enciphering of voice transmissions in a radio communication system **in which signaling on the control channel is conducted in a clear (unciphered) mode.**

Therefore, given that the Sasuta patent relates to a problem that would not arise in the system described by Talbot (because the "control" channel in Talbot's system is not ciphered), it is the Applicant's view that the skilled person would not be motivated to combine the teachings of Sasuta and Talbot as proposed by the Examiner.

Furthermore, should the skilled person attempt to combine the teachings of Sasuta with those of Talbot, the combination would not lead to the invention currently claimed in independent claims 19, 59, 82, 85, 94, 122, 132, 136, and 156. In fact, it is the Applicant's view that the most likely outcome of such an attempted combination would be a system with an encrypted control channel, encryption parameters for the control channel being synchronized as proposed by Sasuta, and in which the allocation of encryption codes and the mechanism for switching between clear and enciphered modes for voice communications (communication on a "working channel" in Sasuta's terminology) would be implemented as proposed by Talbot. This system would be totally different from that currently claimed in independent claims 19, 59, 82, 85, 94, 122, 132, 136, and 156. Any other combination derived from the teachings of Sasuta and Talbot, especially one rendering the presently claimed invention obvious, would require the exercise of inventive ability.

Furthermore, it is also the Applicant's view that Talbot does not provide any teaching concerning the indication of a ciphering mode. This is the feature admitted by the Examiner to be missing from the disclosure of Sasuta and which is sought from the teachings of Talbot in order to render independent claims 19, 59, 82, 85, 94, 122, 132, 136, and 156 obvious. The Examiner refers to the following passages of text in Talbot as evidence that Talbot discloses indication of an enciphering mode: **column 11, line 59 to column 12, line 3; column 8, lines 3 to 25 and column 9, lines 39 to 50.**

Considering the first of these passages, the text between column 11, line 59 and column 12, line 3 discloses that "*the terminal 21 can record the existence of the secure connection so that both parties can be **billed for the added service**, or only the party*

requesting secure voice service can be billed". It should be noted that the "terminal 21" referred to in the referenced section of text is located in a base station of a communication network (see Figure 1, for example). Referring to the final element of newly amended claim 19, this requires: *"...indicating to a user of the mobile station that the mobile **communication network is operating in an enciphered mode of communication, using a cipher mode indicator provided in the mobile station**"* (emphasis added). Therefore, even if billing information is considered to be "an indication" in the sense intended by the claim (an interpretation which the Applicant considers unreasonably broad), in Talbot such an indication is not "provided in the mobile station" as required by claim 19.

A similar argument also applies to newly amended independent apparatus claim 59. This claim relates to "apparatus for use **in a mobile station**...." Thus, all elements of the claim, including the claimed "cipher mode indicator", should be understood as being intended for use **in a mobile station**. Again, this is not what Talbot teaches. Claims 82, 85, 132 and 136 are mobile station claims, all of which require that the claimed mobile station comprises a cipher mode indicator. Thus, the same argument also applies to claims 82, 85, 132 and 136. Similarly, newly amended independent system claim 94, requires "a cipher mode indicator **in the mobile station**", so the same argument again applies. Independent apparatus claim 122 has been amended to clarify that the claimed apparatus is "for use in a mobile station". Thus, the elements of the claim should be interpreted as being intended for use in a mobile station, as explained in connection with independent claim 59. Finally, claim 156 is also directed towards "apparatus for use in a mobile station", so the arguments made with respect to claim 59 also apply to this claim.

Furthermore, it should also be appreciated that the recording of billing information, as disclosed by column 11, line 59 to column 12, line 3 of the Talbot patent, is in no way analogous to an indication of an enciphering mode in the sense intended by the currently pending independent claims. Referring specifically to the wording of claim 19, billing

information cannot provide an indication that a mobile communication network "***is operating in an enciphered mode of communication***", since the billing information referred to in the Talbot patent would only be provided to the user at a later date, usually some (considerable) time after the particular communication to which the billing information relates. While the billing information may reveal that a particular communication, made at some point in the past, ***was*** enciphered, this cannot be equated with an indication that a mobile communication network **is operating in an enciphered mode** e.g. during call set up / while a communication is actually taking place / in connection with a handover between base-stations or different parts of a communication network. Similar arguments apply when considering the language used in the other independent claims (59, 82, 85, 94, 122, 132, 136, and 156).

Thus, the skilled person would appreciate that provision of billing information at a later date does not fulfill the stated purpose of the present invention, namely to ensure that a user of a mobile station is made aware of the security of a particular communication **at the time** the communication is made. For this reason, the skilled person would not consider the teachings of the Talbot patent suitable for combination with Sasuta in order to fulfill the stated aim of the present invention and would have no motivation to attempt the combination.

Should the skilled person still attempt the combination, even without motivation to do so, the resulting system would be quite different from the presently claimed invention. In this respect, it is the Applicant's view that a probable result of combining the teachings of Sasuta with those of Talbot would be a system with an encrypted control channel in which encryption parameters for the control channel would be synchronized as proposed by Sasuta, and in which billing information would be provided as taught by Talbot. This system would not have the characterizing features of the invention presently claimed in independent claims 19, 59, 82, 85, 94, 122, 132, 136 and 156, and would not render the presently claimed invention obvious. Any other combination

derived from the teachings of Sasuta and Talbot would require the exercise of inventive ability.

Turning now to column 8, lines 3 to 25 of the Talbot patent, as referenced by the Examiner, this section of text describes operation of a mobile station in the Talbot system. In particular, column 8, lines 17 to 25 state that "*whenever enciphered voice data is being received, deciphering portion 61....*" (that is the deciphering portion of the mobile station) "*....provides a deciphered output therefrom as well as a signal indicating the presence of the deciphered data. Logic device 59 detects the deciphered data presence signal and in response thereto provides the secure control signal to switch control 65 causing switch 67 to interconnect the output of the enciphering portion 63 with the input to transmitter 55*". As argued in response to previous Official Actions, a mobile station implemented according to the Talbot patent **does not** provide an indication to a user of the mobile station that a particular communication is enciphered. As evidenced by the section of column 8 recited above, if enciphered voice data is received by the mobile station, the deciphering portion automatically provides a deciphered output and the transmitting part of the mobile station is also switched to an enciphered mode of transmission. The "deciphered data presence signal" referred to in the cited text is therefore entirely internal to the functioning of the receiver / transmitter in the mobile station and is not used to provide any form of indication that can be discerned by a user of the device.

To re-iterate, Talbot, like Sasuta, lacks any teaching concerning the provision of an indication of a ciphering mode to a user of the mobile station and therefore any attempted combination of Sasuta with Talbot based on the teaching of column 8, line 3 to 25 would not lead to the solution of the presently claimed invention. The Applicant is of the view that should any such combination be attempted by the skilled person a probable result would be a system comprising a secure control channel in which control channel encryption parameters would be updated according to the teachings of Sasuta and switching between unciphered and enciphered communications on the "working

channels" would be conducted as described in Talbot. This is not the same as the presently claimed invention. Any other combination would require reworking of one or both of the systems according to Sasuta and Talbot and could not be achieved without the exercise of inventive ability.

Finally, the section of text of Talbot in column 9 between lines 39 and 50, cited by the Examiner, describes a mechanism for allowing a user to decide whether communication in a secure mode is desired. As described in the referenced section of text, the terminal 21 (i.e. in the communication network) *"may wait for a secure service request signal from a calling or called party before supplying the secure control signal. This request permits system users to decide if a secure mode and its consequent higher billing expense, is desired"* (column 9, lines 45 to 50). Here it should again be appreciated that the secure control signal is a signal internal to the communication system that controls switching into a secure mode of transmission. Furthermore, the "secure service request signal" is a command issued by either the calling or the called party to indicate that **that party desires** the communication to be conducted in a secure mode. It should be appreciated that this **is not an indication that the communication is actually being conducted in a secure mode**, as in the presently claimed invention. Thus, the system described by Talbot actually suffers from the problem identified in the present application, namely that the user cannot be sure of the security of communication, even if requesting a secure mode when a call is set up – In Talbot's system, if a user of a mobile station moves to a region of the network where enciphered modes of communication are not supported, there is no way for the user to know that the communication is not enciphered (i.e. the communication is insecure) because Talbot does not provide the user with any indication that a given communication is being conducted in secure mode.

Again it is the Applicant's view that any attempted combination of Talbot with Sasuta based on the teachings of column 9, lines 39 to 50 would not give rise to a communication system with the features of the currently claimed invention. The

probable outcome of such a combination would be a communication system with a secure control channel in which control channel encryption parameters would be updated according to the teachings of Sasuta and users would be able to specify the use of either secure or non-secure communication modes on the "working channels" as described in Talbot. This is not the same as the presently claimed invention. Any other combination would require reworking of one or both of the systems according to Sasuta and Talbot and could not be achieved without the exercise of inventive ability.

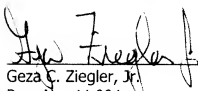
At least for the aforementioned reasons, the Applicant believes the currently claimed invention to be patentably distinct from any combination of Talbot with Sasuta and respectfully requests reconsideration of the application.

The rejections applied to some of the claims, wherein additional references are applied in combination with Sasuta and Talbot, are believed to be overcome in view of the foregoing argumentation against the combination of the teachings of Sasuta and Talbot.

For all of the foregoing reasons, it is respectfully submitted that all of the claims now present in the application are clearly novel and patentable over the prior art of record, and are in proper form for allowance. Accordingly, favorable reconsideration and allowance is respectfully requested. Should any unresolved issues remain, the Examiner is invited to call Applicants' attorney at the telephone number indicated below.

The Commissioner is hereby authorized to charge payment for any fees associated with this communication or credit any over payment to Deposit Account No. 16-1350.

Respectfully submitted,



Geza C. Ziegler, Jr.
Reg. No. 44,004

5 AUGUST 2009
Date

Perman & Green, LLP
425 Post Road
Fairfield, CT 06824
(203) 259-1800
Customer No.: 2512